REMARKS

In the Office Action mailed September 9, 2004, the Examiner noted that claims 1-22 are pending, objected to claims 3 and 13 and rejected claims 1,2, 4-12 and 14-22. Claims 1, 3-11 and 13-22 have been amended. Claims 2 and 12 have been canceled, and new claims 23 and 24 have been added. Thus, in view of the foregoing, claims 1, 3-11 and 13-24 are pending for consideration, which is requested. No new matter has been added. The Examiner's rejections are traversed below.

1. Claim Objections

At item 1 of the Office Action, claims 4 and 14 have been objected to because of informalities. Applicants have amended these claims to correct the informalities.

2. 35 U.S.C. §102 Rejection

At item 4 of the outstanding Office Action, claims 1, 2, 11, 12, 21 and 22 have been rejected under 35 U.S.C. §102(a) as being anticipated by European Pat. No. 1001398, issued to Kanda *et al.* (hereinafter Kanda). See Office Action, at Page 2. The Examiner has alleged that Kanda teaches all elements of independent claim 1.

To minimize estimating a secret key from an extended key, a ciphering algorithm should be secure. Generally, the more the number of nonlinear transformations of a secret key, the more difficult it is to obtain the secret key from an extended key. As the number of extended keys to be prepared increases, however, the number of required linear transformations also increases as more secret keys are processed. As a result, preparing an extended key can result in low processing speed when using conventional ciphering systems, as non-linear transformation is typically performed a specified number of times for each extended key in its entirety.

Kanda teaches an encryption device for concealing data in data communication or storage. The encryption device utilizes a "secret-key algorithm" which encrypts or decrypts data in blocks using a secret key. *See* Kanda, page 2, paragraph 0001.

The present invention, as defined by newly amended independent claims 1, 11, 21 and 22, is directed toward an extended key preparing apparatus wherein extended keys are prepared in common key cryptosystem from a cryptographic key input. The invention allows extended keys to be safely processed at high speeds. *See* Specification, page 3, lines 15-20.

The apparatus includes a dividing unit, an intermediate data preparing unit, a selecting unit, and an extended key preparing unit. *See* Specification, page 3, line 21 – page 4, line 17.

In the present invention, to prepare an extended key, first, the dividing unit divides the bit string of the key into a plurality of bit groups. *See* Specification, page 4, lines 18-21. The intermediate data preparing unit prepares a plurality of intermediate data groups, for example, the twelve items ai, bi, ci, and di, as shown in FIG. 4 of the specification of the present invention. *See also* Specification, page 4, lines 21-23. After the intermediate data groups are prepared, for each of the intermediate data groups, the selecting unit selects a number of elements from the particular data group. The selected number depends on an extended key number r. For example, using the process illustrated in FIG. 5, there are 108 results, that is, 108 extended keys, resulting from the selection by the selecting unit.

The present invention performs non-linear transformation on an intermediate data group the number of times specified for each extended key. For example, if there are 108 extended keys, and non-linear transformation should be performed three times, after the intermediate data groups are prepared, the present invention performs non-linear transformation *on a particular intermediate data group* of each extended key three times, for example, thereby resulting in only thirty-six nonlinear transformations (12 intermediate data items in a group multiplied by three, the number of times non-linear transformation should be performed for each extended key in the example above) and high processing speed of the apparatus. In other words, the non-linear transformation is performed on a particular *intermediate data group* of a given extended key, thereby still resulting in 108 secure extended keys. In addition, in the present invention, the length of the output bit string, that is, the length of an extended key, is greater than the length of the input bit string, that is, the length of the intermediate data group, on which linear transformation will be applied.

Thus, as defined by newly amended independent claim 1, for example, the present invention is directed toward,

> a dividing unit which divides ~~binary digit~~ a bit string of said cryptographic key into a plurality of ~~elements each composed of~~ bit groups, each bit group having a predetermined bit length;
>
> an intermediate data preparing unit which prepares a plurality of intermediate data ~~by applying a plurality of times an operation wherein a predetermined constant is used to the respective elements divided by said dividing unit~~groups from the bit groups by a predetermined operation with different constant for each bit group, each intermediate data group having first intermediate data;

> a selecting unit which selects ~~a plurality of~~ one item of the first intermediate data ~~corresponding to the number of stages of extended keys from the plurality of the intermediate data prepared by said intermediate data preparing unit~~for each of the intermediate data groups depending on a number of stages of extended keys to determine second intermediate data; and
>
> an extended key preparing unit which prepares the extended keys ~~corresponding to said number of stages~~ having a bit length longer than the bit string of said cryptographic key by converting irreversibly the ~~plurality of the~~ second intermediate data ~~selected by said selecting unit.~~, wherein said intermediate data preparing unit is provided with a nonlinear type operating unit for **effecting a nonlinear type operation with respect to each bit group to prepare the intermediate data groups [bold emphasis added]**.

By its language, 35 U.S.C. §102 requires that each and every element of a claim be present in a single cited reference to properly have the reference anticipate the claim. *See In re Bond*, 910 F.2d 831, 15 USPQ2d 1566, 1567 (Fed. Cir. 1992), *citing Diversitech Corp. v. Century Steps, Inc.*, 850 F.2d 675,677, 7 USPQ2d 1315, 1317 (Fed. Cir. 1988); *Lindemann Maschinenfabrik v. American Hoist & Derrick Co.*, 730 F.2d 1452, 1458, 221 USPQ 481, 485 (Fed. Cir. 1984); *Minnesota Mining & Manufacturing Co. v. Johnson & Johnson Orthopaedics, Inc.*, 976 F.2d 1559, 24 USPQ2d 1321, 1326 (Fed. Cir. 1992); and *Elmer v. ICC Fabricating Inc.*, 67 F.3d 1571, 36 USPQ2d 1417, 1419 (Fed. Cir. 1995).

Applicants respectfully submit that the cited reference Kanda does not teach each and every element of the present invention, as defined by newly amended independent claim 1, for example. Unlike the present invention, Kanda does not teach,

> an intermediate data preparing unit which prepares a plurality of intermediate data ~~by applying a plurality of times an operation wherein a predetermined constant is used to the respective elements divided by said dividing unit~~groups from the bit groups by a predetermined operation with different constant for each bit group, each intermediate data group having first intermediate data;
>
> a selecting unit which selects ~~a plurality of~~ one item of the first intermediate data ~~corresponding to the number of stages of extended keys from the plurality of the intermediate data prepared by said intermediate data preparing unit~~for each of the intermediate data groups depending on a number of stages of extended keys to determine second intermediate data; and
>
> an extended key preparing unit which prepares the extended keys ~~corresponding to said number of stages~~ having a bit length longer than the bit string of said cryptographic key by

converting irreversibly the ~~plurality of the~~ second intermediate data ~~selected by said selecting unit.~~, wherein said intermediate data preparing unit is provided with a nonlinear type operating unit for **effecting a nonlinear type operation with respect to each bit group to prepare the intermediate data groups** **[bold emphasis added]**

Although the encryption device of Kanda includes non-linear transformation parts that perform non-linear transformation according to the number of keys, unlike the present invention in which non-linear transformation is performed *on each intermediate data group* (for example, 12 intermediate data items in a group multiplied by three, the number of times non-linear transformation should be performed for each extended key, results in only 36 non-linear transformations, which reduces processing time), thereby resulting in high processing speed of the apparatus, Kanda performs non-linear transformation on *each of the generated extended keys in its entirety.* In a conventional apparatus such as Kanda, non-linear transformation would be performed for each of the extended keys (for example, 108 extended keys multiplied by three, the number of times non-linear transformation should be performed for each extended key results in 324 non-linear transformations), thereby resulting in low processing speed of the apparatus.

In addition, in Kanda, if there are three pieces of output data, for example, mid_{10}, mid_{11}, mid_{12}, and mid_{13}, that is, three generated extended keys, each of the pieces of output data are non-linearly transformed to corresponding pieces of data out_0, out_1, out_2 and out_3. *See* Kanda, page 6, lines 55-58. Thus, unlike the present invention in which the length of an output bit string, that is, the length of an extended key, is larger than a length of an input bit string, that is, the length of an intermediate data group, in Kanda, the length of an output bit string, that is, the length of a generated extended key, is the same as the length of the input bit string, that is, the length of the extended key to be processed by performing linear transformation.

For the reasons set forth above, it is submitted that newly amended independent claims 1, 11, 21, and 22 are properly allowable (claims 11, 21, and 22 recite language similar to that of independent claim 1). Dependent claims 2 and 4-10 depend from independent claim 1 and are thus allowable for at least the reasons offered above with respect to claim 1. Claims 13-20 directly or indirectly depend from independent claim 11and are also properly allowable for at least the reasons offered above with respect to claim 11.

3. 35 U.S.C. §103 Rejection over Kanda in view of Vanstone *et al.*

At item 6 of the Office Action, claims 4-7 and 14-17 have been rejected as being unpatentable over Kanda, and further in view of Vanstone *et al.* (hereinafter Vanstone).

Applicants respectfully submit that unlike the present invention, Vanstone does not teach or suggest, "an intermediate data preparing unit which prepares a plurality of intermediate data groups . . . wherein said intermediate data preparing unit is provided with a nonlinear type operating unit for **effecting a nonlinear type operation with respect to each bit group to prepare the intermediate data groups [bold emphasis added]**," according to the language recited in claims 4-7 via claim 1. Vanstone also does not teach, "a selecting unit which selects one item of the first intermediate data" according to the language recited in claim1.

Rather, Vanstone merely teaches a block cipher that encrypts plaintext in fixed-sized *n*-bit blocks. Although messages exceeding *n* bits are partitioned into *n*-bit blocks, ***each*** *n*-bit block is encrypted separately in its entirety. Applicants submit that encrypting ***each*** *n*-bit block can result in lower ciphering time. In light of the foregoing, claim 4 is patentable over Kanda in view of Vanstone, as neither Kanda nor Vanstone, taken alone, or in combination, teaches or suggests the features identified by the above-quoted language of claim 4 as recited via its independent claim 1. Claims 14-17 recite language similar to claims 4-7 and are thus patentable over Kanda in view of Vanstone, for at least the reason offered above with respect to claims 4-7.

4. 35 U.S.C. §103 Rejection over Kanda in view of Ohmori *et al.*

At item 7 of the Office Action, claims 8, 9, 18, and 19 have been rejected as being unpatentable over Kanda, and further in view of Ohmori *et al.* (hereinafter Ohmori). Applicants respectfully submit that unlike the present invention, Ohmori does not teach or suggest, "an intermediate data preparing unit which prepares **a plurality of intermediate data groups from the bit groups**," according to the language recited in claims 8 and 9 via independent claim 1 and in claims 18 and 19 via independent claim 11. Ohmori also does not teach or suggest, "a selecting unit which selects one item of the first intermediate data" according to the language recited in the above referenced independent claims.

As described above, Kanda teaches encryption of the entire key and does not select data groups from the key. Ohmori teaches a cryptographic processing apparatus including a data encrypting apparatus which encrypts plaintext data in units of 64 bits using 256-bit key data and 8K-bit substitution data. Thus, the substitution data is not selected from the extended key data. Rather, the substitution data is separate data that is retrieved from a table. See Ohmori, column 11, lines 31-34.

Therefore, Applicants submit that claims 8-9 and 18-19 are patentable over Kanda in view of Ohmori as neither of the references, taken alone, or in combination teach the feature

identified by the above quoted language in the independent claims from which the dependent claims 8-9 and 18-19 depend.

5. Allowable Subject Matter

At item 9 of the Office Action, claims 3 and 13 have been objected to as being dependent upon a rejected base claim. Accordingly, Applicants have included the subject matter of each of these dependent claims 3 and 13, including all of the limitations of the base claim and any intervening claims, in new independent claims 23 and 24, respectively.

It is submitted that claims 1-24 are allowable. It is further submitted that the features recited by the language of the claims are not taught or suggested by the references. The claims are therefore in a condition suitable for allowance. An early Notice of Allowance is requested.

If any further fees, other than and except for the issue fee, are necessary with respect to this paper, the U.S.P.T.O. is requested to obtain the same from deposit account number 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 1/7/4

By: _____

J. Randall Beckers
Registration No. 30,358

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501